

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-083297

(43)Date of publication of application : 31.03.1998

(51)Int.Cl.

G06F 9/06

G06F 12/14

(21)Application number : 09-120523 (71)Applicant : FUJITSU LTD

(22)Date of filing : 12.05.1997 (72)Inventor : AKIYAMA RYOTA  
YOSHIOKA MAKOTO  
UCHIDA YOSHIKI

(30)Priority

Priority number : 08124823 Priority date : 20.05.1996 Priority country : JP

(54) PROCESSOR AND METHOD FOR SOFTWARE COPY PROCESSING AND  
COMPUTER-READABLE RECORDING MEDIUM WHERE PROGRAM FOR  
COPYING SOFTWARE IS RECORDED

(57)Abstract:

PROBLEM TO BE SOLVED: To formally copy copyright protected software stored on a master medium to a user's storage medium as to the software copy processor.

SOLUTION: A content identifier read means 2 reads the identifier of software on the master medium 1 and a storage medium identifier read means 4 reads the identifier of the copy destination storage medium 3; and they are sent to a center 5 which administers copyright vending. The center 5 generates a signature from the information of the sent identifier by a signature generating means 6 and sends it to the user. The sent signature is written on the copy destination storage medium 3 by a signature write means 7. A signature generating and comparing means 8 generates a signature on the user side from the information of the identifier sent to the center and compares this generated signature with the signature written on the copy destination storage medium 3 and only when the signatures match each other a data copy means 9 reads the copy object software out of the master medium 1 and copies it to the copy destination storage medium 3.

CLAIMS

---

[Claim(s)]

[Claim 1] A software copy processing device which copies software recorded on a master medium to a copy destination storage comprising:

A content identifier reading means which reads information on the 1st identifier according to software individual recorded on a master medium corresponding to each software.

A storage-medium-identifiers reading means which reads information on the 2nd identifier individually recorded for every copy destination storage.

A signature generating means to generate the 1st signature that attested a right of a copy of copy object software in response to information on the 1st and 2nd identifiers that said content identifier reading means and said storage-medium-identifiers reading means read in a center which manages sale of a right of a copy respectively.

A signature writing means which writes said 1st signature generated in said signature generating means in said copy destination storage. While said content identifier reading means and said storage-medium-identifiers reading means generate the 2nd signature for verification from information on said 1st and 2nd identifiers read respectively. A signature generating comparison means to judge whether the 1st signature written in said copy destination storage is read and it is in agreement as compared with said 2nd signature. A data copy means which reads copy object software in a master medium and is written in a copy destination storage as a result of comparison in said signature generating comparison means when the 1st and 2nd signatures are in agreement.

[Claim 2] The software copy processing device comprising according to claim 1:

A signature processing means which outputs an attestation child who enciphered information on said 1st and 2nd identifiers that said content identifier reading means and said storage-medium-identifiers reading means read said signature generating means respectively with an authentication key which a center has managed as said 1st signature.

An encoding means which enciphers an authentication key used by said signature processing means with a user individual key registered into said center and is outputted with said attestation child.

[Claim 3] The software copy processing device comprising according to claim 2:

A decoding means which said signature generating comparison means decodes an authentication key enciphered by said signature generating means with a user individual key registered into said center and outputs an authentication key.

An attestation child creating means which enciphers information on the 1st and 2nd identifiers that said content identifier reading means and said storage-medium-identifiers reading means read respectively with an authentication key which said decoding means decoded and outputs an attestation child for verification as said 2nd signature.

A comparison means to compare an attestation child for said verification with an attestation child written in said copy destination storage as the 1st signature.

[Claim 4] In a software copy processing method which copies software recorded on a master medium to a copy destination storage, a content identifier of copy object data recorded on a master medium and storage medium identifiers peculiar to a copy destination storage are sent to a center which sells a right of a copy from an end user together with right demand information of a copy. While carrying out signature processing for said content identifier and storage medium identifiers which were received in said center with an authentication key of a center and generating the 1st attestation child, carry out encryption processing of said authentication key with a user individual key, and an encrypted authentication key is generated. The 1st [ said ] attestation child and encrypted authentication key that were generated are sent to an end user. The 1st [ said ] attestation child and encrypted authentication key that won popularity in an end user are written in said copy destination storage. An authentication key which carried out decoding processing of the encrypted authentication key written in said copy destination storage with a user individual key and was enciphered in said center is acquired. Carry out signature processing of said content identifier and the storage medium identifiers using a decoded authentication key, generate the 2nd attestation child for verification, and the 2nd attestation child for generated verification is compared with said 1st attestation child written in said copy destination storage. A software copy processing method which consists of what copy object data of said master medium is read and is written in said copy destination storage when the 1st [ said ] attestation child written in said copy destination storage and the 2nd attestation child for said verification are in agreement.

[Claim 5] A software copy processing device which copies software recorded on a master medium to a copy destination storage, comprising:

A content identifier reading means which reads information on the 1st identifier according to software individual recorded on a master medium corresponding to each software.

A storage-medium-identifiers reading means which reads information on the 2nd identifier individually recorded for every copy destination storage.

A conversion key for master media is generated from information on the 2nd identifier that said storage-medium-identifiers reading means read while generating a conversion key for storages from information on the 1st identifier that said content identifier reading means read in a center which manages sale of a right of a copy. A conversion key generating means which enciphers said conversion key for storages and a conversion key for master media which were generated for information on said 2nd identifier.

A conversion key writing means which writes a conversion key for encryption storages outputted from said conversion key generating means in said copy destination storage. A conversion key decoding means which carries out decoding processing of a conversion key for encryption storages and a conversion key for

encryption master media which were outputted from said conversion key generating means for information on said 2nd identifier that said storage-medium-identifiers reading means readA data decryption means to read copy object software recorded on said master medium to decode with said conversion key for master media decoded by said conversion key decoding means and to output data of a plaintextA data writing means which enciphers data of said plaintext with said conversion key for storages decoded by said conversion key decoding means and is written in said copy destination storage.

[Claim 6]The software copy processing device comprising according to claim 5:  
The 1st encoding means that said conversion key generating means enciphers information on the 1st identifier that said content identifier reading means read with a master key which a center has managed and generates a conversion key for storages.

The 2nd encoding means that enciphers information on the 2nd identifier that said storage-medium-identifiers reading means read with said master key and generates a conversion key for master media.

The 3rd encoding means that enciphers said conversion key for storages and a conversion key for master media for information on said 2nd identifier.

[Claim 7]In a software copy processing method which copies software which is enciphered with a conversion key for master media made from a content identifier which identifies software and a master key which a center which sells a right of a copy has managed and is recorded on a master medium to a copy destination storageA content identifier of copy object data recorded on a master medium and storage medium identifiers peculiar to a copy destination storage are sent to said center from an end userEncipher said content identifier and storage medium identifiers which were received in said center with a master key of a center and a conversion key for master media and a conversion key for storages are generatedSaid conversion key for master media and a conversion key for storages are enciphered by said storage medium identifiers respectivelySaid conversion key for master media and a conversion key for storages which were enciphered are sent to an end userA conversion key for encryption storages which won popularity in an end user is written in said copy destination storageDecode a conversion key for encryption master media and a conversion key for encryption storages which won popularity by said storage medium identifiers decode copy object data of said master medium with said conversion key for master media make it data of a plaintext and data of said plaintext is enciphered with said conversion key for storagesA software copy processing method which consists of what enciphered data is written for in said copy destination storage.

[Claim 8]A content identifier reading means which reads information on the 1st identifier according to software individually recorded on a master medium in a computer corresponding to each softwareA storage-medium-identifiers reading means which reads information on the 2nd identifier individually recorded for every

copy destination storageA delivery means which sends information on the 1st and 2nd identifiers that said content identifier reading means and said storage-medium-identifiers reading means readrespectively to a center which manages sale of a right of a copyA reception means which receives the 1st signature that attested a right of a copy of copy object software generated from information on said 1st and 2nd identifiers from said centerA signature writing means which writes said 1st signature received from said center in said copy destination storageWhile said content identifier reading means and said storage-medium-identifiers reading means generate the 2nd signature for verification from information on said 1st and 2nd identifiers readrespectively. A result of comparison in a signature generating comparison means to judge whether the 1st signature written in said copy destination storage is readand it is in agreement as compared with said 2nd signatureand said signature generating comparison meansA recording medium which recorded a program for making it function as a data copy means which reads copy object software in a master mediumand is written in a copy destination storage when the 1st and 2nd signatures are in agreement and in which computer reading is possible.

[Claim 9]A content identifier reading means which reads information on the 1st identifier according to software individual recorded on a master medium in a computer corresponding to each softwareA storage-medium-identifiers reading means which reads information on the 2nd identifier individually recorded for every copy destination storageA delivery means which sends information on the 1st and 2nd identifiers that said content identifier reading means and said storage-medium-identifiers reading means readrespectively to a center which manages sale of a right of a copyA reception means which receives a conversion key for encryption storages and a conversion key for encryption master media which enciphered a conversion key for master media generated from information on a conversion key for storages generated from information on the 1st identifierand the 2nd identifier for information on said 2nd identifier from said centerA conversion key writing means which writes said conversion key for encryption storages in said copy destination storageA conversion key decoding means which carries out decoding processing of said conversion key for encryption storagesand the conversion key for encryption master media for information on said 2nd identifier that said storage-medium-identifiers reading means readA data decryption means to read copy object software recorded on said master mediumto decode with said conversion key for master media decoded by said conversion key decoding meansand to output data of a plaintextAnd a recording medium which recorded a program for making it function as a data writing means which enciphers data of said plaintext with said conversion key for storages decoded by said conversion key decoding meansand is written in said copy destination storage and in which computer reading is possible.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is about the recording medium which records the program which copies a software copy processing device, the software copy processing method, and software in which computer reading is possible. It is related with the recording medium which records the program which copies the software copy processing device, the software copy processing method, and software which copy especially copyright protection software to a user's storage justly and in which computer reading is possible.

[0002] Some circulation forms of software are various and in recent years a floppy disk and CD-ROM (compact disk read only memory). Although what records software on storage, such as semiconductor memory, may be purchased or it may be purchased by downloading software via a network. All of such software are usually serious about the software which always has a problem of an illegal copy in other storages and has copyright in them easily since it can copy.

[0003]

[Description of the Prior Art] Conventionally, there is the method of recording and distributing these software to CD-ROM in the state where it is locked electronically. One of the sales styles of the software of the application program for computers is dictionary data, an image, music data, etc. In this case, a user does purchase procedure of software to connect and use for the center which has managed sale of that software. Then the user can install it on a hard disk by opening software with a key using the key passed at the time of purchase procedure.

[0004] The identifier information about the right sale of a copy which the center has managed beforehand may be written in the storage which can be written in as another example. When copying the software recorded on CD-ROM, the store or user of the storage notifies to a center. Only when in agreement as compared with the identifier information in which the identifier information published from a center by carrying out sales procedure of software was written by the storage, it becomes possible to copy software to a storage from CD-ROM.

[0005]

[Problem(s) to be Solved by the Invention] However, the software installed on the hard disk etc. could usually be performed or used as it was, namely, since it was not locked, the problem of an illegal copy still had the problem of not being canceled.

[0006] When identifier information was written in the storage, the center needed to cooperate with the factory which manufactures a storage, needed to manage identifier information, and moreover had the problem that it was necessary to distinguish and deal with the medium only for a copy and the storage for general about a storage.

[0007] This invention is made in view of such a point and is a thing.

the purpose can copy justly the software with copyright boiled and memorized to the storage with a medium identifier of the user in whom read/write is possible --

and[ software copy processing ] It is providing the recording medium which recorded the program which copies the software copy processing method and software and in which computer reading is possible.

[0008]

[Means for Solving the Problem]Drawing 1 is a principle figure of this invention which attains the above-mentioned purpose. A software copy processing device of this invention comprises:

The content identifier reading means 2 which reads an identifier of copy object software recorded on the master medium 1.

The storage-medium-identifiers reading means 4 which reads an identifier of the copy destination storage 3.

A signature generating means 6 to generate a signature which attested a right of a copy to a user who demanded a right of a copy from information on an identifier which the content identifier reading means 2 and the storage-medium-identifiers reading means 4 read in the center 5 which manages sale of a right of a copy.

The signature writing means 7 which writes a generated signature in the copy destination storage 3. A signature generating comparison means 8 to compare a signature written in the copy destination storage 3 with a signature generated by the user side and a data copy means 9 to copy copy object software of the master medium 1 to the copy destination storage 3 when a comparison result is in agreement.

[0009]According to the above-mentioned composition first the content identifier reading means 2 reads a content identifier of software in the master medium 1 and the storage-medium-identifiers reading means 4 reads the storage medium identifiers in the copy destination storage 3. Information on these identifiers is sent to a center. In the center 5 the signature generating means 6 generates a signature from information on a sent identifier and it returns to a user. The signature is written in the copy destination storage 3 by the signature writing means 7. The signature generating comparison means 8 is compared with a signature which generated a signature internally from information on an identifier read by the content identifier reading means 2 and the storage-medium-identifiers reading means 4 and was written in the copy destination storage 3. When comparison of this signature is in agreement the data copy means 9 copies copy object software enciphered from the master medium 1 to the copy destination storage 3 as it is.

[0010]In a software copy processing method which copies software recorded on a master medium to a copy destination storage according to this invention a content identifier of copy object data recorded on a master medium and storage medium identifiers peculiar to a copy destination storage are sent to a center which sells a right of a copy from an end user together with right demand information of a copy. While carrying out signature processing for said content identifier and storage medium identifiers which were received in said center with an authentication key

of a center and generating the 1st attestation child carry out encryption processing of said authentication key with a user individual key and an encrypted authentication key is generated. The 1st [ said ] attestation child and encrypted authentication key that were generated are sent to an end user. The 1st [ said ] attestation child and encrypted authentication key that won popularity in an end user are written in said copy destination storage. An authentication key which carried out decoding processing of the encrypted authentication key written in said copy destination storage with a user individual key and was enciphered in said center is acquired. Carry out signature processing of said content identifier and the storage medium identifiers using a decoded authentication key, generate the 2nd attestation child for verification and the 2nd attestation child for generated verification is compared with said 1st attestation child written in said copy destination storage. When the 1st [ said ] attestation child written in said copy destination storage and the 2nd attestation child for said verification are in agreement, a software copy processing method which consists of what copy object data of said master medium is read and is written in said copy destination storage is provided.

[0011] A content identifier reading means which reads information on the 1st identifier according to software individual recorded on a master medium in a computer corresponding to each software according to this invention. A storage-medium-identifiers reading means which reads information on the 2nd identifier individually recorded for every copy destination storage. A delivery means which sends information on the 1st and 2nd identifiers that said content identifier reading means and said storage-medium-identifiers reading means read respectively to a center which manages sale of a right of a copy. A reception means which receives the 1st signature that attested a right of a copy of copy object software generated from information on said 1st and 2nd identifiers from said center. A signature writing means which writes said 1st signature received from said center in said copy destination storage. While said content identifier reading means and said storage-medium-identifiers reading means generate the 2nd signature for verification from information on said 1st and 2nd identifiers read respectively. A result of comparison in a signature generating comparison means to judge whether the 1st signature written in said copy destination storage is read and it is in agreement as compared with said 2nd signature and said signature generating comparison means. When the 1st and 2nd signatures are in agreement, a recording medium which recorded a program for making it function as a data copy means which reads copy object software in a master medium and is written in a copy destination storage and in which computer reading is possible is provided.

[0012] This recording medium can be preferably used as a master medium which is recording software and the same medium. Information on the 1st identifier according to software individual is read in a master medium because a computer reads and performs a content identifier reading means from a recording medium. Information on the 2nd identifier individually recorded by the storage-



medium-identifiers reading means 4 for every copy destination storage from a copy destination storage is read. Information on these identifiers is sent to a center which manages sale of a right of a copy by a delivery means. Then if the 1st signature that attested a right of a copy of software from a center by a reception means is received a signature writing means will write the 1st signature in a copy destination storage. Next it compares with the 1st signature that generated the 2nd signature internally from information on the 1st and 2nd identifiers and was written in a copy destination storage by a signature generating comparison means. When these signatures are in agreement software is copied to a copy destination storage from a master medium by a data copy means.

[0013]

[Embodiment of the Invention] First the outline of this invention is explained with reference to drawings. Drawing 1 is a figure showing the principle composition of the software copy processing device of this invention.

[0014] In this figure the software copy processing device of this invention comprises the following:

The content identifier reading means 2 which reads the identification information according to software individual of the copy object software recorded on the master medium 1.

The storage-medium-identifiers reading means 4 which reads the individual identification information of the copy destination storage 3.

A signature generating means 6 to generate the signature which attested the right of a copy of copy object software in response to the identification information which the content identifier reading means 2 and the storage-medium-identifiers reading means 4 read in the center 5 which manages sale of the right of a copy respectively.

The signature writing means 7 which writes the signature generated by this signature generating means 6 in the copy destination storage 3. A signature generating comparison means 8 to judge whether the content identifier reading means 2 and the storage-medium-identifiers reading means 4 generate a signature from the identification information read respectively and this is compared with the signature written in the copy destination storage 3 and it is in agreement. The data copy means 9 which reads the copy object software in the master medium 1 and is written in the copy destination storage 3 when a signature is in agreement by this signature generating comparison means 8.

[0015] The software of a selling object is enciphered the master medium 1 is recorded and the content identifier is attached to each software. The copy destination storage 3 assumes that individual storage medium identifiers are beforehand attached at the time of the factory shipments. If a user specifies copy object software here out of the software currently recorded on the master medium 1 the content identifier reading means 2 reads the content identifier corresponding to the software in the master medium 1 and the storage-medium-identifiers reading means 4 reads the storage medium identifiers in the copy

destination storage 3. The information on these identifiers is sent to the center 5 together with the demand of the right purchase of a copy. In the center 5 the signature which attested the right of a copy is generated from the information on the content identifier which the signature generating means 6 received and storage medium identifiers and it returns to a user. The center 5 performs a user's registration processing and accounting to a user profile again in the case of signature generating.

[0016] In the user side the signature writing means 7 writes this in the copy destination storage 3 in response to the signature sent from the signature generating means 6. Subsequently in the signature generating comparison means 8 a signature is first generated internally from the content identifier read by the content identifier reading means 2 and the storage medium identifiers read by the storage-medium-identifiers reading means 4. Next it is judged whether this generated signature is compared with the signature written in the copy destination storage 3 and it is in agreement. When comparison of the signature in the signature generating comparison means 8 is in agreement the data copy means 9 reads the copy object software enciphered from the master medium 1 and writes in the copy destination storage 3. When a user uses the software written in the copy destination storage 3 it will develop and perform to the main memory of the processing unit which performs this software decoding that software.

[0017] Next the case where the copyright protection software among which the embodiment of the invention was distributed in CD-ROM is copied to MO (magneto-optical disc; magneto-optical disc) medium is made into an example and it explains.

[0018] Drawing 2 is a flow chart which shows the flow of processing of a software copy processing device. In copying the software recorded on CD-ROM to MO media in the software copy processing device of this invention First the software individual identifier SID<sub>i</sub> of software which wishes the storage individual identifier ID<sub>k</sub> of MO media and the copy of CD-ROM in the end user side is transmitted to the center which has managed sale of the right of a copy (Step S1).

Subsequently in the center side while performing procedure processing of the right sale of a copy attestation child CS is generated from the received storage individual identifier ID<sub>k</sub> and the software individual identifier SID<sub>i</sub> and it returns to the end user side (Step S2). In the end user side attestation child CS which received is written in the predetermined storage area of MO media (Step S3).

Attestation child CS' for verification is generated using the storage individual identifier ID<sub>k</sub> and the software individual identifier SID<sub>i</sub> which transmitted to the center here at the end user side (step S4). And attestation child CS' generated by the end user side is compared with attestation child CS written in MO media (Step S5). The encryption data of the software which it is judged whether both attestation children are in agreement as a result of comparison of these attestation child CS' and CS (Step S6) and has the software individual identifier SID<sub>i</sub> from CD-ROM when in agreement here is written in MO media (Step S7). When both attestation children are not in agreement with Step S6 in a judgment it

ends without performing the writing of the software from CD-ROM to MO media. [0019] Drawing 3 is a figure showing the composition of CD-ROM and MO media. In this figure (A) is the composition of CD-ROM 11 what was shown and to this CD-ROM 11. Manager application software MA which performs copy operation of the copyright protection software which has the software individual identifier  $SID_i$  ( $i=12\dots n$ ) respectively and the copyright protection software from CD-ROM to MO media is recorded. Each copyright protection software is recorded in the state where it was enciphered respectively. When copying software to MO media from CD-ROM manager application software MA is read into the main part of a terminal like the end user side for example a personal computer is performed and performs processing of end users among processings of drawing 2.

[0020] (B) is what showed the composition of MO media 12 and the storage individual identifier  $ID_k$  ( $k=12\dots m$ ) is recorded on these MO media 12. Rewriting is an impossible field although the field where the storage individual identifier  $ID_k$  of MO media 12 is written in although as for MO media 12 the user has a storage area which can write in data freely or can be eliminated is possible for read-out. This storage individual identifier  $ID_k$  can be made into the serial number attached to each MO media for example at the time of factory shipments.

[0021] Next the concrete procedure which copies the copyright protection software of CD-ROM to MO media is explained. Drawing 4 is a figure showing the procedure of the copy processing of copyright protection software.

[0022] The procedure of copy processing is divided into the processing by the side of the main part of composition and the processing by the side of the center which has managed sale of the right of a copy for example with a personal computer this figure is shown and it is the main part side here. [End user] Center side A [center] shows and it is between them. [The channel/haulageway] has shown.

[0023] The terminal of an end user is provided with a CD-ROM drive device and an MO drive device and here to a CD-ROM drive device. It shall be loaded with CD-ROM 11 which is the master medium with which copyright protection software was recorded and the MO drive device shall be loaded with MO media 12 which are media of a copy destination. And the copy object software of CD-ROM 11 is software which has the software individual identifier  $SID_i$  and an identifier peculiar to MO media 12 presupposes that it is the storage individual identifier  $ID_k$ .

[0024] First manager application software MA of CD-ROM 11 is started in the main part side processing of an end user. If copy object software is specified the software individual identifier  $SID_i$  of the software will be read in CD-ROM 11 and the storage individual identifier  $ID_k$  will be read in MO media 12. These software individual identifier  $SID_i$  and the storage individual identifier  $ID_k$  are transmitted to a center with a request sentence including the right demand information of a copy.

[0025] In the center side the request content of the information from the end user which received is first written in the user profile 13. The software individual identifier  $SID_i$  which received and the storage individual identifier  $ID_k$  are inputted into the signature processing unit 14. This signature processing unit 14 performs data compression processing using the authentication key  $KEY_c$  of the center

which is a secret key and outputs attestation child CS. This attestation child CS plays the role of a signature. Next it is inputted into the enciphering device 15 and is enciphered with the user individual key KU and the authentication key KEYc used with the signature processing unit 14 is outputted as the encryption wording of a telegram ECU (KEYc). The encryption wording of a telegram ECU (KEYc) outputted from attestation child CS and the enciphering device 15 which were outputted from the signature processing unit 14 is returned to an end user with the center identifier IDc.

[0026] In the end user side attestation child CS and the encryption wording of a telegram ECU (KEYc) are once written in on MO media 12 of a copy destination among the information sent from the center. And attestation child CS and the encryption wording of a telegram ECU (KEYc) on this written-in medium are passed to manager application.

[0027] In the main part side processing the authentication key KEYc enciphered in the center is taken out by inputting the passed encryption wording of a telegram ECU (KEYc) into the decoding device 16 and decoding it first using the user individual key KU for signature verification. Subsequently from the storage individual identifier IDk read in the software individual identifier SIDI read in CD-ROM 11 and MO media 12 in the signature processing unit 17. Attestation child CS' for verification is generated by the end user side using the authentication key KEYc decoded in the decoding device 16. Then attestation child CS written in on MO media 12 and attestation child CS' generated with the signature processing unit 17 are compared by the comparator 18. If attestation child CS and attestation child CS' is in agreement as a result of comparison by the comparator 18 the switch 19 will operate and the copy object software which has the software individual identifier SIDI will be written in MO media 12 of a copy destination in the state of encryption data.

[0028] Here the example of the processing in the signature processing unit 14 by the side of a center and the signature processing unit 17 of end users is explained below. Drawing 5 is a figure showing the constructional example of a signature processing unit.

[0029] The exclusive OR treating part 21 to which a signature processing unit performs exclusive OR processing in response to the software individual identifier SIDI and the storage individual identifier IDk and attestation child CS. It consists of the enciphering processing part 22 which inputs the output of this exclusive OR treating part 21 and the authentication key KEYc of a center and outputs attestation child CS and the hash function is constituted.

[0030] First the software individual identifier SIDI and storage individual identifier IDk data which were inputted are enciphered by the authentication key KEYc by a block unit in the enciphering processing part 22. It returns to an input side exclusive OR processing is carried out with the following block data in the exclusive OR treating part 21 and the output data by which encryption processing was carried out by the enciphering processing part 22 is again enciphered by the enciphering processing part 22. Such processing is repeated until the last block is

inputted. In the meantime a processing result is not outputted but when a final block is enciphered it is outputted as attestation child CS for the first time from the enciphering processing part 22.

[0031] Next the procedure in the case of executing the program of the software included in the data copied while it had been enciphered by MO media 12 in the above procedure is explained.

[0032] Drawing 6 is an explanatory view showing the executive operation procedure of the program of the software included in the copied data. Attestation child CS the encryption wording of a telegram E<sub>KU</sub> (KEY<sub>c</sub>) storage individual identifier ID<sub>k</sub> data and the software individual identifier SID<sub>i</sub> are recorded on MO media 12 and the copied software is recorded on them as the encryption data E<sub>Kd</sub> (DATA). When this encryption data E<sub>Kd</sub> (DATA) records software on CD-ROM 11 it is enciphered with the key K<sub>d</sub> and the key K<sub>d</sub> used for that encryption is held by manager application software.

[0033] In the main part side processing first Attestation child CS from MO media 12 the encryption wording of a telegram E<sub>KU</sub> (KEY<sub>c</sub>) Storage individual identifier ID<sub>k</sub> data and the software individual identifier SID<sub>i</sub> are read the encryption wording of a telegram E<sub>KU</sub> (KEY<sub>c</sub>) of them is inputted into the decoding device 16 and the authentication key KEY<sub>c</sub> is taken out by being decoded using the user individual key K<sub>U</sub>. Subsequently attestation child CS' for verification is generated using the authentication key KEY<sub>c</sub> decoded in the decoding device 16 in the storage individual identifier ID<sub>k</sub> read in the software individual identifier SID<sub>i</sub> read from MO media 12 and MO media 12. Then attestation child CS written in on MO media 12 and attestation child CS' generated by the signature processing unit 17 are compared by the comparator 18. If attestation child CS and attestation child CS' is in agreement as a result of comparison by the comparator 18 the switch 19 will operate and the encryption data E<sub>Kd</sub> (DATA) which is the encryption software read from MO media 12 will be inputted into the decoding device 25 via the switch 19. In the decoding device 25 the inputted encryption data E<sub>Kd</sub> (DATA) is decoded using the key K<sub>d</sub> which manager application software holds and is returned to data DAT A of a plaintext. This data DAT A is loaded on the memory of the central processing unit (CPU) and the memory 26 by the side of a main part and executive operation of the program of that software is carried out by CPU here.

[0034] Next another embodiment of the software copy processing device of this invention is described. In this example the software recorded on CD-ROM has software individual identifier DID and the data Data of the software is enciphered with the conversion key K<sub>a</sub> for master media made from software individual identifier DID and the master key K<sub>M</sub> which the right sales center of a copy has managed. Assuming that it is the encryption data E<sub>Ka</sub> (Data) MO media assume that it has a serial number of the storage individual identifier Mid.

[0035] Drawing 7 is a flow chart which shows the flow of another copy processing of a software copy processing device. First software individual identifier DID of software which wishes the storage individual identifier Mid of the MO media of a copy destination and the copy of CD-ROM in the end user side is transmitted to

the right sales center of a copy which has managed sale of the right of a copy (Step S11). Subsequently in the center side verification of whether received software individual identifier DID is registered into the center is performed (Step S12). Then it enciphers with the master key KM of center management of the storage individual identifier Mid and software individual identifier DID which were received and the conversion key Ku for storages and the conversion key Ka for master media are generated (Step S13). Subsequently the conversion key Ku for these storages and the conversion key Ka for master media are enciphered by the storage individual identifier Mid and the encryption wording of a telegram EMid (KuKa) which generated and generated the encryption wording of a telegram EMid (KuKa) is returned to the end user of a requiring agency (Step S14). The inside of the encryption wording of a telegram EMid (KuKa) which received in the end user side The encryption wording of a telegram EMid (KuKa) which received while writing the encryption wording of a telegram EMid (Ku) which has the information relevant to MO media in MO media is decoded by the storage individual identifier Mid and the conversion key Ku for storages and the conversion key Ka for master media are obtained (Step S15). Next the conversion key Ka for master media obtained at Step S15 is used the encryption data EKa (Data) corresponding to software individual identifier DID of CD-ROM is decoded and the data Data of a plaintext is obtained (Step S16). And this data Data is re-enciphered with the conversion key Ku for storages obtained at Step S15 it writes in MO media and a copy is ended (Step S17).

[0036] Next the concrete procedure which copies the software of CD-ROM to MO media is explained. The processing first performed when giving a demand to the right sales center of a copy by the end user side The reading processing of software individual identifier DID of the storage individual identifier Mid of the MO media of a copy destination and the copy object software of CD-ROM Since it is only transmitting processing to the center of these storage individual identifier Mid and software individual identifier DID the explanation about this first processing is omitted and is performed from explanation of processing by the side of a center.

[0037] Drawing 8 is an explanatory view showing the procedure of the processing by the side of a center. In this figure a center receives first the storage individual identifier Mid and software individual identifier DID which were transmitted from the end user through the circuit Among these it inputs into the enciphering device 31 which has the master key KM of center management of the storage individual identifier Mid and software individual identifier DID is inputted into the comparator 32. The enciphering device 31 enciphers the storage individual identifier Mid with the master key KM and generates the conversion key Ku for storages. On the other hand for justification verification of software individual identifier DID the comparator 32 searches the issue content identifier file 33 and compares it with demanded software individual identifier DID. Here the switch 34 is controlled by the closed state when software individual identifier DID required as software individual identifier DID of the issue content identifier file 33 is in agreement. Then demanded software individual identifier DID is inputted into the enciphering device 35 which

has the master key KM. The enciphering device 35 enciphers software individual identifier DID with the master key KM and generates the conversion key Ka for master media. The conversion key Ka for master media generated with the conversion key Ku for storages and the enciphering device 35 which were generated with the enciphering device 31 is inputted into the enciphering device 36 and is enciphered by the storage individual identifier Mid respectively. The encryption wording of a telegram EMid (KuKa) enciphered by the enciphering device 36 is transmitted to the end user of a requiring agency through a circuit. If this processing is attained, directions of accounting will be told to the user profile 37 and fee collection will be carried out to the end user of a requiring agency.

[0038] Drawing 9 is an explanatory view showing the procedure of processing of end users. In this figure, reception of the encryption wording of a telegram EMid (KuKa) transmitted from the center will write the encryption wording of a telegram EMid about the MO media of them (Ku) in the predetermined field 41 of MO media 40 first. And the received encryption wording of a telegram EMid (KuKa) is inputted into the decoding device 51. The decoding device 51 decodes the encryption wording of a telegram EMid (KuKa) using the storage individual identifier Mid of MO media 40 and outputs the conversion key Ku for storages and the conversion key Ka for master media. The decoded conversion key Ka for master media is inputted into the decoding device 52 as a decode key and the conversion key Ku for storages is inputted into the enciphering device 53 as an encryption key. First, the decoding device 52 reads the encryption data EKa (Data) corresponding to software individual identifier DID of CD-ROM 60 and decodes it with the conversion key Ka for master media and is returned and outputted to the data Data of a plaintext. This data Data is inputted into the enciphering device 53 and is re-enciphered with the conversion key Ku for storages. The encryption data EKu (Data) enciphered with the enciphering device 53 is written in MO media 40.

[0039] Next, the procedure in the case of using the encryption data EKu (Data) based on an identifier peculiar to these MO media 40 and the conversion key based on the master key of a center written in MO media 40 in the above procedure is explained.

[0040] Drawing 10 is an explanatory view showing the use procedure of the copied data. The encryption wording of a telegram EMid (Ku) is memorized to the field 41 in the field which can rewrite MO media 40; the storage individual identifier Mid is memorized to the field 42 which is not rewritable and the encryption data EKu (Data) copied to a part of other field is memorized. Here, when using the encryption data EKu (Data), first, the storage individual identifier Mid on MO media 40 and the encryption wording of a telegram EMid (Ku) are read and it is inputted into the decoding device 54. The decoding device 54 decodes the encryption wording of a telegram EMid (Ku) using the storage individual identifier Mid and outputs the conversion key Ku for storages. The decoding device 55 uses the conversion key Ku for storages as a decode key, decodes the encryption data EKu (Data) read from MO media 40 and outputs the data Data of a plaintext. It is developed on the main memory of the personal computer which is a terminal of an end user; this data Data

will be performed if this is a program and if it is dictionary data it will be searched and used.

[0041]

[Effect of the Invention] As explained above, the center side is equipped with a signature generating means to generate a signature from the information on the identifier of the copy object data of a master medium and the identifier of a copy destination storage in this invention. The signature writing means which writes the signature generated by the signature generating means in the end user side in a copy destination storage. It is constituted so that it might have a signature generating comparison means to compare the signature for verification generated by the end user side with the signature written in the copy destination storage and a data copy means which writes the copy object data of a master medium in a copy destination storage by a comparison result. For this reason, the center should just publish a corresponding signature with this to the information on the identifier of a copy destination storage. Management of the identifier information which cooperates with the plant of a copy destination storage is also unnecessary and it can make inventory management of a copy destination storage unnecessary in the store which sells the factory which manufactures a copy destination storage and this.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is a figure showing the principle composition of the software copy processing device of this invention.

[Drawing 2] It is a flow chart which shows the flow of processing of a software copy processing device.

[Drawing 3] It is a figure showing the composition of CD-ROM and MO media.

[Drawing 4] It is a figure showing the procedure of the copy processing of copyright protection software.

[Drawing 5] It is a figure showing the constructional example of a signature processing unit.

[Drawing 6] It is an explanatory view showing the executive operation procedure of the program of the software included in the copied data.

[Drawing 7] It is a flow chart which shows the flow of another copy processing of a software copy processing device.

[Drawing 8] It is an explanatory view showing the procedure of the processing by the side of a center.

[Drawing 9] It is an explanatory view showing the procedure of processing of end users.

[Drawing 10] It is an explanatory view showing the use procedure of the copied data.

[Description of Notations]



- 1 Master medium
  - 2 Content identifier reading means
  - 3 Copy destination storage
  - 4 Storage-medium-identifiers reading means
  - 5 Center
  - 6 Signature generating means
  - 7 Signature writing means
  - 8 Signature generating comparison means
  - 9 Data copy means
-

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-83297

(43) 公開日 平成10年(1998) 3月31日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 G
12/14	3 2 0		12/14	3 2 0 E

審査請求 未請求 請求項の数 9 O L (全 11 頁)

(21) 出願番号 特願平9-120523

(22) 出願日 平成9年(1997) 5月12日

(31) 優先権主張番号 特願平8-124823

(32) 優先日 平8(1996) 5月20日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72) 発明者 秋山 良太

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(72) 発明者 吉岡 誠

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(72) 発明者 内田 好昭

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

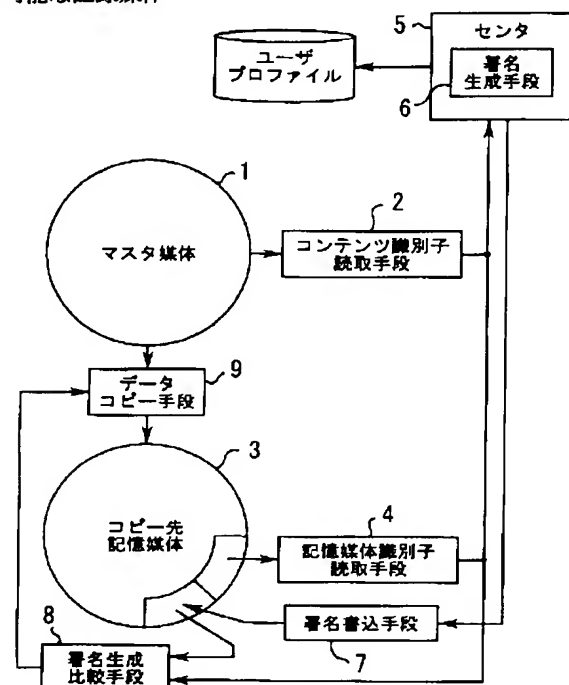
(74) 代理人 弁理士 服部 毅巖

(54) 【発明の名称】 ソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 ソフトウェアコピー処理装置に関し、マスタ媒体に記憶された著作権保護ソフトウェアをユーザの記憶媒体に正当にコピーできるようにすることを目的とする。

【解決手段】 コンテンツ識別子読取手段2がマスタ媒体1上のソフトウェアの識別子を、記憶媒体識別子読取手段4がコピー先記憶媒体3の識別子をそれぞれ読み取り、コピー権販売を管理するセンタ5に送る。センタ5では署名生成手段6が送られた識別子の情報から署名を生成し、ユーザに送る。送られた署名は署名書込手段7によりコピー先記憶媒体3に書き込まれる。署名生成比較手段8はセンタ5に送った識別子の情報からユーザ側で署名を生成し、この生成した署名とコピー先記憶媒体3に書き込まれた署名とを比較し、署名が一致した場合のみ、データコピー手段9がマスタ媒体1のコピー対象ソフトウェアを読み出してコピー先記憶媒体3にコピーする。



## 【特許請求の範囲】

【請求項1】 マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理装置において、

個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段と、

コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段と、

コピー権の販売を管理するセンタにおいて前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別子の情報を受けてコピー対象ソフトウェアのコピー権を認証した第1の署名を生成する署名生成手段と、

前記署名生成手段において生成された前記第1の署名を前記コピー先記憶媒体に書き込む署名書込手段と、

前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第1および第2の識別子の情報から検証用の第2の署名を生成するとともに前記コピー先記憶媒体に書き込まれた第1の署名を読み出して前記第2の署名と比較して一致するかどうかを判定する署名生成比較手段と、

前記署名生成比較手段における比較の結果、第1および第2の署名が一致した場合にマスタ媒体におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体に書き込むデータコピー手段とを備えていることを特徴とするソフトウェアコピー処理装置。

【請求項2】 前記署名生成手段は、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第1および第2の識別子の情報をセンタが管理している認証鍵で暗号化した認証子を前記第1の署名として出力する署名処理手段と、前記署名処理手段で使用された認証鍵を前記センタに登録されているユーザ個別鍵で暗号化して前記認証子とともに出力する暗号化手段とを有していることを特徴とする請求項1記載のソフトウェアコピー処理装置。

【請求項3】 前記署名生成比較手段は、前記署名生成手段にて暗号化された認証鍵を前記センタに登録したユーザ個別鍵で復号して認証鍵を出力する復号手段と、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別子の情報を前記復号手段が復号した認証鍵で暗号化して検証用の認証子を前記第2の署名として出力する認証子生成手段と、前記検証用の認証子と前記コピー先記憶媒体に第1の署名として書き込まれた認証子とを比較する比較手段とを有することを特徴とする請求項2記載のソフトウェアコピー処理装置。

【請求項4】 マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理方法において、

マスタ媒体に記録されたコピー対象データのコンテンツ識別子とコピー先記憶媒体に固有の記憶媒体識別子とをコピー権要求情報と一緒にエンドユーザからコピー権を販売するセンタに送り、

前記センタでは受けた前記コンテンツ識別子および記憶媒体識別子をセンタの認証鍵にて署名処理をして第1の認証子を生成するとともに前記認証鍵をユーザ個別鍵で暗号化処理して暗号化認証鍵を生成し、

生成された前記第1の認証子および暗号化認証鍵をエンドユーザに送り、

エンドユーザでは受けた前記第1の認証子および暗号化認証鍵を前記コピー先記憶媒体に書き込み、

前記コピー先記憶媒体に書き込まれた暗号化認証鍵をユーザ個別鍵で復号処理して前記センタで暗号化された認証鍵を取得し、

復号された認証鍵を使って前記コンテンツ識別子と記憶媒体識別子とを署名処理して検証用の第2の認証子を生成し、

生成された検証用の第2の認証子と前記コピー先記憶媒体に書き込まれた前記第1の認証子とを比較し、

前記コピー先記憶媒体に書き込まれた前記第1の認証子と前記検証用の第2の認証子とが一致した場合に、前記マスタ媒体のコピー対象データを読み出して前記コピー先記憶媒体に書き込む、

ことからなるソフトウェアコピー処理方法。

【請求項5】 マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理装置において、

個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段と、

コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段と、

コピー権の販売を管理するセンタにおいて前記コンテンツ識別子読取手段が読み取った第1の識別子の情報から記憶媒体用変換鍵を生成するとともに前記記憶媒体識別子読取手段が読み取った第2の識別子の情報からマスタ媒体用変換鍵を生成し、生成した前記記憶媒体用変換鍵およびマスタ媒体用変換鍵を前記第2の識別子の情報で暗号化する変換鍵生成手段と、

前記変換鍵生成手段より出力された暗号化記憶媒体用変換鍵を前記コピー先記憶媒体に書き込む変換鍵書込手段と、

前記変換鍵生成手段より出力された暗号化記憶媒体用変換鍵および暗号化マスタ媒体用変換鍵を前記記憶媒体識別子読取手段が読み取った前記第2の識別子の情報で復号処理する変換鍵復号手段と、

前記マスタ媒体に記録されたコピー対象ソフトウェアを読み出し、前記変換鍵復号手段で復号された前記マスタ媒体用変換鍵で復号して平文のデータを出力するデータ

復号手段と、  
前記平文のデータを前記変換鍵復号手段で復号された前記記憶媒体用変換鍵で暗号化して前記コピー先記憶媒体に書き込むデータ書込手段と、  
を備えていることを特徴とするソフトウェアコピー処理装置。

【請求項6】 前記変換鍵生成手段は、前記コンテンツ識別子読取手段が読み取った第1の識別子の情報をセンタが管理しているマスタ鍵で暗号化して記憶媒体用変換鍵を生成する第1の暗号化手段と、前記記憶媒体識別子読取手段が読み取った第2の識別子の情報を前記マスタ鍵で暗号化してマスタ媒体用変換鍵を生成する第2の暗号化手段と、前記記憶媒体用変換鍵およびマスタ媒体用変換鍵を前記第2の識別子の情報で暗号化する第3の暗号化手段とを有することを特徴とする請求項5記載のソフトウェアコピー処理装置。

【請求項7】 ソフトウェアを識別するコンテンツ識別子とコピー権を販売するセンタが管理しているマスタ鍵とから作られたマスタ媒体用変換鍵によって暗号化されてマスタ媒体に記録されているソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理方法において、  
マスタ媒体に記録されたコピー対象データのコンテンツ識別子とコピー先記憶媒体に固有の記憶媒体識別子とをエンドユーザから前記センタに送り、  
前記センタでは受けた前記コンテンツ識別子および記憶媒体識別子をセンタのマスタ鍵で暗号化してマスタ媒体用変換鍵および記憶媒体用変換鍵を生成し、  
前記マスタ媒体用変換鍵および記憶媒体用変換鍵をそれぞれ前記記憶媒体識別子で暗号化し、  
暗号化された前記マスタ媒体用変換鍵および記憶媒体用変換鍵をエンドユーザに送り、  
エンドユーザでは受けた暗号化記憶媒体用変換鍵を前記コピー先記憶媒体に書き込み、  
受けた暗号化マスタ媒体用変換鍵および暗号化記憶媒体用変換鍵を前記記憶媒体識別子で復号し、  
前記マスタ媒体のコピー対象データを前記マスタ媒体用変換鍵で復号して平文のデータにし、  
前記平文のデータを前記記憶媒体用変換鍵で暗号化し、  
暗号化されたデータを前記コピー先記憶媒体に書き込む、  
ことからなるソフトウェアコピー処理方法。

【請求項8】 コンピュータを、  
個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段、  
コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段、  
前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別

子の情報をコピー権の販売を管理するセンタに送る送出手段、

前記第1および第2の識別子の情報から生成されたコピー対象ソフトウェアのコピー権を認証した第1の署名を前記センタから受け取る受信手段、

前記センタから受け取った前記第1の署名を前記コピー先記憶媒体に書き込む署名書込手段、

前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第1および第2の識別子の情報から検証用の第2の署名を生成するとともに前記コピー先記憶媒体に書き込まれた第1の署名を読み出して前記第2の署名と比較して一致するかどうかを判定する署名生成比較手段、および前記署名生成比較手段における比較の結果、第1および第2の署名が一致した場合にマスタ媒体におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体に書き込むデータコピー手段として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項9】 コンピュータを、  
個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段、

コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段、

前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別子の情報をコピー権の販売を管理するセンタに送る送出手段、

第1の識別子の情報から生成された記憶媒体用変換鍵および第2の識別子の情報から生成されたマスタ媒体用変換鍵を前記第2の識別子の情報で暗号化した暗号化記憶媒体用変換鍵および暗号化マスタ媒体用変換鍵を前記センタから受け取る受信手段、

前記暗号化記憶媒体用変換鍵を前記コピー先記憶媒体に書き込む変換鍵書込手段、

前記暗号化記憶媒体用変換鍵および暗号化マスタ媒体用変換鍵を前記記憶媒体識別子読取手段が読み取った前記第2の識別子の情報で復号処理する変換鍵復号手段、

前記マスタ媒体に記録されたコピー対象ソフトウェアを読み出し、前記変換鍵復号手段で復号された前記マスタ媒体用変換鍵で復号して平文のデータを出力するデータ復号手段、および前記平文のデータを前記変換鍵復号手段で復号された前記記憶媒体用変換鍵で暗号化して前記コピー先記憶媒体に書き込むデータ書込手段として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウ

ウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特に著作権保護ソフトウェアをユーザの記憶媒体に正当にコピーするソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】近年、ソフトウェアの流通形態には様々のもがあり、フロッピーディスクやCD-ROM(compact disk read only memory)、半導体メモリなどの記憶媒体にソフトウェアを記録したものを購入したり、あるいはネットワークを経由してソフトウェアをダウンロードすることによって購入したりする場合があるが、これらのソフトウェアは通常いずれも他の記憶媒体に容易にコピーが可能のため、常に不正コピーの問題があり、著作権のあるソフトウェアについては深刻である。

【0003】

【従来の技術】従来、コンピュータ用のアプリケーションプログラム、辞書データ、映像・音楽データなどのソフトウェアの販売形態の一つに、これらソフトウェアをCD-ROMに電子的に鍵をかけた状態で記録して頒布する方法がある。この場合、ユーザは、そのソフトウェアの販売を管理しているセンタに連絡して利用したいソフトウェアの購入手続きをする。その後、ユーザは、購入手続き時に渡された鍵を使って鍵付きのソフトウェアを開くことにより、それをたとえばハードディスクにインストールすることができる。

【0004】また、別の例として、書き込み可能な記憶媒体にあらかじめセンタが管理しているコピー権販売に関する識別子情報を書き込んでおく場合がある。CD-ROMに記録されたソフトウェアをコピーする場合は、その記憶媒体の販売店またはユーザがセンタに通知する。ソフトウェアの販売手続きをすることによってセンタから発行される識別子情報を記憶媒体に書き込まれた識別子情報と比較して一致する場合のみ、CD-ROMから記憶媒体にソフトウェアをコピーすることが可能になる。

【0005】

【発明が解決しようとする課題】しかし、ハードディスクなどにインストールされたソフトウェアは、通常、そのまま実行あるいは利用できる、すなわち、鍵がかけていないので、依然として不正コピーの問題は解消されていないという問題点があった。

【0006】また、記憶媒体に識別子情報を書き込んでおく場合には、センタは記憶媒体を製造する工場と連携して識別子情報を管理する必要がある、しかも、記憶媒体についてコピー専用媒体と一般用記憶媒体とを区別して取り扱う必要があるという問題点があった。

【0007】本発明はこのような点に鑑みてなされたものであり、マスタ媒体に記憶された著作権付きのソフト

ウェアをリード/ライト可能なユーザの媒体識別子付き記憶媒体に正当にコピーすることができるソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】図1は上記目的を達成する本発明の原理図である。本発明のソフトウェアコピー処理装置は、マスタ媒体1に記録されたコピー対象ソフトウェアの識別子を読み取るコンテンツ識別子読取手段2と、コピー先記憶媒体3の識別子を読み取る記憶媒体識別子読取手段4と、コピー権の販売を管理するセンタ5においてコンテンツ識別子読取手段2および記憶媒体識別子読取手段4が読み取った識別子の情報からコピー権を要求したユーザにコピー権を認証した署名を生成する署名生成手段6と、生成された署名をコピー先記憶媒体3に書き込む署名書込手段7と、コピー先記憶媒体3に書き込まれた署名とユーザ側で生成した署名とを比較する署名生成比較手段8と、比較結果が一致した場合にマスタ媒体1のコピー対象ソフトウェアをコピー先記憶媒体3にコピーするデータコピー手段9とから構成されている。

【0009】上記の構成によれば、まず、コンテンツ識別子読取手段2がマスタ媒体1からソフトウェアのコンテンツ識別子を読み取り、記憶媒体識別子読取手段4がコピー先記憶媒体3からその記憶媒体識別子を読み取る。これらの識別子の情報は、センタに送られる。センタ5では、送られた識別子の情報から署名生成手段6が署名を生成してユーザに送り返す。その署名は、署名書込手段7によりコピー先記憶媒体3に書き込まれる。署名生成比較手段8は、コンテンツ識別子読取手段2および記憶媒体識別子読取手段4で読み取った識別子の情報から内部的に署名を生成してコピー先記憶媒体3に書き込まれた署名と比較する。この署名の比較が一致した場合は、データコピー手段9がマスタ媒体1から暗号化されたコピー対象ソフトウェアをそのままコピー先記憶媒体3にコピーする。

【0010】また、本発明によれば、マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理方法において、マスタ媒体に記録されたコピー対象データのコンテンツ識別子とコピー先記憶媒体に固有の記憶媒体識別子とをコピー権要求情報と一緒にエンドユーザからコピー権を販売するセンタに送り、前記センタでは受けた前記コンテンツ識別子および記憶媒体識別子をセンタの認証鍵にて署名処理をして第1の認証子を生成するとともに前記認証鍵をユーザ個別鍵で暗号化処理して暗号化認証鍵を生成し、生成された前記第1の認証子および暗号化認証鍵をエンドユーザに送り、エンドユーザでは受けた前記第1の認証子およ

び暗号化認証鍵を前記コピー先記憶媒体に書き込み、前記コピー先記憶媒体に書き込まれた暗号化認証鍵をユーザ個別鍵で復号処理して前記センタで暗号化された認証鍵を取得し、復号された認証鍵を使って前記コンテンツ識別子と記憶媒体識別子とを署名処理して検証用の第2の認証子を生成し、生成された検証用の第2の認証子と前記コピー先記憶媒体に書き込まれた前記第1の認証子とを比較し、前記コピー先記憶媒体に書き込まれた前記第1の認証子と前記検証用の第2の認証子とが一致した場合に、前記マスタ媒体のコピー対象データを読み出して前記コピー先記憶媒体に書き込む、ことからなるソフトウェアコピー処理方法が提供される。

【0011】さらに、本発明によれば、コンピュータを、個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段、コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別子の情報をコピー権の販売を管理するセンタに送る送出手段、前記第1および第2の識別子の情報から生成されたコピー対象ソフトウェアのコピー権を認証した第1の署名を前記センタから受け取る受信手段、前記センタから受け取った前記第1の署名を前記コピー先記憶媒体に書き込む署名書込手段、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第1および第2の識別子の情報から検証用の第2の署名を生成するとともに前記コピー先記憶媒体に書き込まれた第1の署名を読み出して前記第2の署名と比較して一致するかどうかを判定する署名生成比較手段、および前記署名生成比較手段における比較の結果、第1および第2の署名が一致した場合にマスタ媒体におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体に書き込むデータコピー手段として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【0012】この記録媒体は、好ましくは、ソフトウェアを記録しているマスタ媒体と同じ媒体とすることができる。コンピュータが記録媒体からコンテンツ識別子読取手段を読み出して実行することでマスタ媒体からソフトウェア個別の第1の識別子の情報が読み取られ、記憶媒体識別子読取手段4によりコピー先記憶媒体からコピー先記憶媒体毎に個別に記録された第2の識別子の情報が読み取られる。これらの識別子の情報は、送出手段によりコピー権の販売を管理するセンタに送られる。続いて、受信手段によりセンタからソフトウェアのコピー権を認証した第1の署名を受け取ると、署名書込手段がその第1の署名をコピー先記憶媒体に書き込む。次に、署名生成比較手段により、第1および第2の識別子の情報から内部的に第2の署名を生成してコピー先記憶媒体に

書き込まれた第1の署名と比較し、これらの署名が一致した場合に、データコピー手段によりソフトウェアをマスタ媒体からコピー先記憶媒体にコピーする。

【0013】

【発明の実施の形態】まず、本発明の概略について図面を参照して説明する。図1は本発明のソフトウェアコピー処理装置の原理構成を示す図である。

【0014】この図において、本発明のソフトウェアコピー処理装置は、マスタ媒体1に記録されたコピー対象ソフトウェアのソフトウェア個別の識別情報を読み取るコンテンツ識別子読取手段2と、コピー先記憶媒体3の個別の識別情報を読み取る記憶媒体識別子読取手段4と、コピー権の販売を管理するセンタ5においてコンテンツ識別子読取手段2および記憶媒体識別子読取手段4がそれぞれ読み取った識別情報を受けてコピー対象ソフトウェアのコピー権を認証した署名を生成する署名生成手段6と、この署名生成手段6で生成された署名をコピー先記憶媒体3に書き込む署名書込手段7と、コンテンツ識別子読取手段2および記憶媒体識別子読取手段4がそれぞれ読み取った識別情報から署名を生成してこれとコピー先記憶媒体3に書き込まれた署名とを比較して一致するかどうかを判定する署名生成比較手段8と、この署名生成比較手段8にて署名が一致した場合にマスタ媒体1におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体3に書き込むデータコピー手段9とから構成されている。

【0015】マスタ媒体1は販売対象のソフトウェアが暗号化されて記録されており、各ソフトウェアにはコンテンツ識別子が付けられている。また、コピー先記憶媒体3はその工場出荷時にあらかじめ個別の記憶媒体識別子が付けられているとする。ここで、ユーザがマスタ媒体1に記録されているソフトウェアの中からコピー対象ソフトウェアを指定すると、コンテンツ識別子読取手段2がマスタ媒体1からそのソフトウェアに対応するコンテンツ識別子を読み取り、記憶媒体識別子読取手段4がコピー先記憶媒体3からその記憶媒体識別子を読み取る。これら識別子の情報はコピー権購入の要求と一緒にセンタ5に送られる。センタ5では、署名生成手段6が受けたコンテンツ識別子および記憶媒体識別子の情報からコピー権を認証した署名を生成して、ユーザに送り返す。センタ5は、また、署名生成の際に、ユーザプロフィールに対してユーザの登録処理および課金処理を行う。

【0016】ユーザ側では、署名書込手段7が署名生成手段6より送られて来た署名を受けて、これをコピー先記憶媒体3に書き込む。次いで、署名生成比較手段8においては、まず、コンテンツ識別子読取手段2により読み取られたコンテンツ識別子と記憶媒体識別子読取手段4により読み取られた記憶媒体識別子とから内部的に署名を生成し、次に、この生成された署名とコピー先記憶

媒体3に書き込まれた署名とを比較して一致しているかどうかを判定する。署名生成比較手段8における署名の比較が一致した場合は、データコピー手段9がマスタ媒体1から暗号化されているコピー対象ソフトウェアを読み取ってコピー先記憶媒体3に書き込む。ユーザがコピー先記憶媒体3に書き込まれたソフトウェアを利用する場合は、そのソフトウェアを復号しながらこのソフトウェアを実行する処理装置のメインメモリに展開して実行することになる。

【0017】次に、本発明の実施の形態を、CD-ROMにて配付された著作権保護ソフトウェアをMO(magneto-optical disc:光磁気ディスク)媒体にコピーする場合を例にして説明する。

【0018】図2はソフトウェアコピー処理装置の処理の流れを示すフローチャートである。本発明のソフトウェアコピー処理装置において、CD-ROMに記録されたソフトウェアをMO媒体にコピーする場合には、まず、エンドユーザ側にて、MO媒体の記憶媒体個別識別子IDkおよびCD-ROMのコピーを希望するソフトウェアのソフトウェア個別識別子SIDiを、コピー権の販売を管理しているセンタに送信する(ステップS1)。次いで、センタ側では、コピー権販売の手続き処理を行うとともに、受信された記憶媒体個別識別子IDkおよびソフトウェア個別識別子SIDiから認証子CSを生成してエンドユーザ側に送り返す(ステップS2)。エンドユーザ側では、受信した認証子CSをMO媒体の所定の記憶領域に書き込む(ステップS3)。ここで、エンドユーザ側においても、センタに送信した記憶媒体個別識別子IDkおよびソフトウェア個別識別子SIDiを使って検信用の認証子CS'を生成する(ステップS4)。そして、エンドユーザ側で生成した認証子CS'とMO媒体に書き込まれた認証子CSとを比較する(ステップS5)。これら認証子CS'およびCSの比較の結果、両認証子が一致しているかどうか判定され(ステップS6)、ここで、一致している場合には、CD-ROMからソフトウェア個別識別子SIDiを有するソフトウェアの暗号化データをMO媒体に書き込む(ステップS7)。もし、ステップS6に判定において、両認証子が一致していない場合には、CD-ROMからMO媒体へのソフトウェアの書き込みは行われずに終了する。

【0019】図3はCD-ROMおよびMO媒体の構成を示す図である。この図において、(A)はCD-ROM11の構成を示したもので、このCD-ROM11には、それぞれソフトウェア個別識別子SIDi(i=1, 2, ..., n)を有する著作権保護ソフトウェアと、CD-ROMからMO媒体への著作権保護ソフトウェアのコピー操作を行うマネージャアプリケーションソフトウェアMAとが記録されている。各著作権保護ソフトウェアはそれぞれ暗号化された状態で記録されてい

る。マネージャアプリケーションソフトウェアMAは、CD-ROMからMO媒体へソフトウェアをコピーする場合に、エンドユーザ側のたとえばパーソナルコンピュータのような端末の本体に読み込まれて実行され、図2の処理のうちエンドユーザ側の処理を行う。

【0020】また、(B)はMO媒体12の構成を示したもので、このMO媒体12には、記憶媒体個別識別子IDk(k=1, 2, ..., m)が記録されている。MO媒体12はユーザが自由にデータを書き込んだり、消去することができる記憶領域を有しているが、MO媒体12の記憶媒体個別識別子IDkが書き込まれている領域は、読み出しは可能であるが書き換えは不可能な領域である。この記憶媒体個別識別子IDkは、たとえば工場出荷時にそれぞれのMO媒体に付けられるシリアル番号とすることができる。

【0021】次に、CD-ROMの著作権保護ソフトウェアをMO媒体にコピーする具体的な手順について説明する。図4は著作権保護ソフトウェアのコピー処理の手順を示す図である。

【0022】この図において、コピー処理の手順を、たとえばパーソナルコンピュータで構成の本体側の処理とコピー権の販売を管理しているセンタ側の処理とに分けて示してあり、ここでは、本体側を〔エンドユーザ〕、センタ側を〔センタ〕で示し、それらの間は〔通信路／運搬路〕で示してある。

【0023】ここで、エンドユーザの端末はCD-ROMドライブ装置およびMOドライブ装置を備え、CD-ROMドライブ装置には、著作権保護ソフトウェアが記録されたマスタ媒体であるCD-ROM11が装填されており、MOドライブ装置にはコピー先の媒体であるMO媒体12が装填されているものとする。そして、CD-ROM11のコピー対象ソフトウェアはソフトウェア個別識別子SIDiを有するソフトウェアであり、MO媒体12に固有の識別子は記憶媒体個別識別子IDkであるとする。

【0024】まず、エンドユーザの本体側処理では、CD-ROM11のマネージャアプリケーションソフトウェアMAを起動して、コピー対象ソフトウェアが指定されると、CD-ROM11からそのソフトウェアのソフトウェア個別識別子SIDiが読み取られ、MO媒体12から記憶媒体個別識別子IDkが読み取られる。これらソフトウェア個別識別子SIDiおよび記憶媒体個別識別子IDkは、コピー権要求情報を含む要求文とともにセンタに送信される。

【0025】センタ側では、受信したエンドユーザからの情報の要求内容をまず、ユーザプロファイル13に書き込む。さらに、受信したソフトウェア個別識別子SIDiおよび記憶媒体個別識別子IDkは署名処理装置14に入力される。この署名処理装置14は、秘密鍵であるセンタの認証鍵KEYcを使ってデータ圧縮処理を行



い、認証子CSを出力する。この認証子CSが署名の役割を果たす。次に、署名処理装置14で使用了認証鍵KEYcは暗号化装置15に力入され、ユーザ個別鍵KUで暗号化されて、暗号化電文EKU (KEYc)として出力される。署名処理装置14より出力された認証子CSおよび暗号化装置15より出力された暗号化電文EKU (KEYc)は、センタ識別子IDcとともにエンドユーザに送り返される。

【0026】エンドユーザ側では、センタより送られた情報のうち、認証子CSおよび暗号化電文EKU (KEYc)はコピー先のMO媒体12上に一度書き込まれ、そしてこの書き込まれた媒体上の認証子CSおよび暗号化電文EKU (KEYc)がマネージャアプリケーションへ渡される。

【0027】本体側処理では、署名検証のために、まず、渡された暗号化電文EKU (KEYc)が復号装置16に力入され、ユーザ個別鍵KUを使用して復号されることにより、センタにおいて暗号化された認証鍵KEYcが取り出される。次いで、署名処理装置17において、CD-ROM11から読み取ったソフトウェア個別識別子SIDiおよびMO媒体12から読み取った記憶媒体個別識別子IDkから、復号装置16において復号された認証鍵KEYcを使って、エンドユーザ側で検証用の認証子CS'を生成する。その後、MO媒体12上に書き込まれた認証子CSと署名処理装置17で生成された認証子CS'とが比較器18で比較される。比較器18での比較の結果、認証子CSと認証子CS'とが一致すれば、スイッチ19が作動して、ソフトウェア個別識別子SIDiを有するコピー対象ソフトウェアが暗号化データの状態で、コピー先のMO媒体12に書き込まれる。

【0028】ここで、センタ側の署名処理装置14およびエンドユーザ側の署名処理装置17における処理の例について以下に説明する。図5は署名処理装置の構造例を示す図である。

【0029】署名処理装置は、ソフトウェア個別識別子SIDiおよび記憶媒体個別識別子IDkと認証子CSとを受けて排他的論理和处理を行う排他的論理和处理部21と、この排他的論理和处理部21の出力とセンタの認証鍵KEYcとを力入して認証子CSを出力する暗号化処理部22とからなり、ハッシュ関数を構成している。

【0030】まず、力入されたソフトウェア個別識別子SIDiおよび記憶媒体個別識別子IDkデータは、暗号化処理部22においてブロック単位で認証鍵KEYcにより暗号化される。暗号化処理部22で暗号化処理された出力データは力入側に帰還されて、排他的論理和处理部21において次のブロックデータと排他的論理和处理され、暗号化処理部22で再び暗号化される。このような処理は、最終のブロックが力入されるまで繰り返さ

れる。この間、処理結果は出力されず、最終ブロックが暗号化されたとき、暗号化処理部22から初めて認証子CSとして出力される。

【0031】次に、以上の手順でMO媒体12に暗号化されたままでコピーされたデータに含まれるソフトウェアのプログラムを実行する場合の処理手順について説明する。

【0032】図6はコピーされたデータに含まれるソフトウェアのプログラムの実行処理手順を示す説明図である。MO媒体12には、認証子CS、暗号化電文EKU (KEYc)、記憶媒体個別識別子IDkデータ、およびソフトウェア個別識別子SIDiが記録され、コピーされたソフトウェアは暗号化データEKd (DATA)として記録されている。この暗号化データEKd (DATA)はソフトウェアをCD-ROM11に記録する際に鍵Kdによって暗号化されたものであり、その暗号化に力用した鍵Kdはマネージャアプリケーションソフトウェアによって保持されている。

【0033】本体側処理では、まず、MO媒体12から認証子CS、暗号化電文EKU (KEYc)、記憶媒体個別識別子IDkデータ、およびソフトウェア個別識別子SIDiが読み出され、その内の暗号化電文EKU (KEYc)が復号装置16に力入され、ユーザ個別鍵KUを使用して復号されることで認証鍵KEYcが取り出される。次いで、MO媒体12から読み出したソフトウェア個別識別子SIDiおよびMO媒体12から読み取った記憶媒体個別識別子IDkを、復号装置16において復号された認証鍵KEYcを使って、検証用の認証子CS'を生成する。その後、MO媒体12上に書き込まれた認証子CSと署名処理装置17によって生成された認証子CS'とが比較器18で比較される。比較器18での比較の結果、認証子CSと認証子CS'とが一致すれば、スイッチ19が作動し、MO媒体12から読み出された暗号化ソフトウェアである暗号化データEKd (DATA)がそのスイッチ19を経由して復号装置25に力入される。復号装置25では、力入された暗号化データEKd (DATA)はマネージャアプリケーションソフトウェアが保持している鍵Kdを使って復号され、平文のデータDATAに戻される。このデータDATAは、本体側の中央処理装置(CPU)・メモリ26のメモリ上にロードされ、ここで、そのソフトウェアのプログラムはCPUによって実行処理される。

【0034】次に、本発明のソフトウェアコピー処理装置の別の実施の形態について説明する。この例では、CD-ROMに記録されたソフトウェアはソフトウェア個別識別子DIDを有し、かつ、そのソフトウェアのデータDataはソフトウェア個別識別子DIDとコピー権販売センタが管理しているマスタ鍵KMとから作られたマスタ媒体用変換鍵Kaによって暗号化され、暗号化データEKa (Data)になっているとし、MO媒体は



記憶媒体個別識別子M i dのシリアル番号を有しているとする。

【0035】図7はソフトウェアコピー処理装置の別のコピー処理の流れを示すフローチャートである。まず、エンドユーザ側にて、コピー先のMO媒体の記憶媒体個別識別子M i dおよびC D-R O Mのコピーを希望するソフトウェアのソフトウェア個別識別子D I Dをコピー権の販売を管理しているコピー権販売センタに送信する（ステップS 11）。次いで、センタ側では、受信されたソフトウェア個別識別子D I Dがセンタに登録されているかどうかの検証が行われる（ステップS 12）。その後、受信された記憶媒体個別識別子M i dおよびソフトウェア個別識別子D I Dをセンタ管理のマスタ鍵K Mで暗号化して記憶媒体用変換鍵K uおよびマスタ媒体用変換鍵K aを生成する（ステップS 13）。次いで、これら記憶媒体用変換鍵K uおよびマスタ媒体用変換鍵K aを記憶媒体個別識別子M i dで暗号化して暗号化電文E M i d（K u，K a）を生成し、生成した暗号化電文E M i d（K u，K a）を要求元のエンドユーザへ送り返す（ステップS 14）。エンドユーザ側では、受信した暗号化電文E M i d（K u，K a）のうち、MO媒体に関連した情報を有する暗号化電文E M i d（K u）をMO媒体に書き込むとともに受信した暗号化電文E M i d（K u，K a）を記憶媒体個別識別子M i dで復号して記憶媒体用変換鍵K uおよびマスタ媒体用変換鍵K aを得る（ステップS 15）。次に、ステップS 15で得られたマスタ媒体用変換鍵K aを使用して、C D-R O Mのソフトウェア個別識別子D I Dに対応する暗号化データE K a（D a t a）を復号し、平文のデータD a t aを得る（ステップS 16）。そして、このデータD a t aをステップS 15で得られた記憶媒体用変換鍵K uで再暗号化してMO媒体に書き込み、コピーを終了する（ステップS 17）。

【0036】次に、C D-R O MのソフトウェアをMO媒体にコピーする具体的な手順について説明する。なお、エンドユーザ側でコピー権販売センタに要求を出すときに最初に行われる処理は、コピー先のMO媒体の記憶媒体個別識別子M i dおよびC D-R O Mのコピー対象ソフトウェアのソフトウェア個別識別子D I Dの読み出し処理と、これら記憶媒体個別識別子M i dおよびソフトウェア個別識別子D I Dのセンタへの送信処理だけなので、この最初の処理に関する説明は省略し、センタ側の処理の説明から行う。

【0037】図8はセンタ側における処理の手順を示す説明図である。この図において、センタは、まず、回線を通じてエンドユーザから送信された記憶媒体個別識別子M i dおよびソフトウェア個別識別子D I Dを受信し、このうち、記憶媒体個別識別子M i dをセンタ管理のマスタ鍵K Mを有する暗号化装置31に入力し、ソフトウェア個別識別子D I Dを比較器32へ入力する。暗

号化装置31は記憶媒体個別識別子M i dをマスタ鍵K Mで暗号化して記憶媒体用変換鍵K uを生成する。一方、比較器32は、ソフトウェア個別識別子D I Dの正当性検証のため、発行コンテンツ識別子ファイル33を検索し、要求されたソフトウェア個別識別子D I Dと比較する。ここで、発行コンテンツ識別子ファイル33のソフトウェア個別識別子D I Dと要求されたソフトウェア個別識別子D I Dとが一致した場合には、スイッチ34は閉成状態に制御される。すると、要求されたソフトウェア個別識別子D I Dはマスタ鍵K Mを有する暗号化装置35に入力される。暗号化装置35はソフトウェア個別識別子D I Dをマスタ鍵K Mで暗号化してマスタ媒体用変換鍵K aを生成する。暗号化装置31で生成された記憶媒体用変換鍵K uおよび暗号化装置35で生成されたマスタ媒体用変換鍵K aは暗号化装置36に入力され、それぞれ記憶媒体個別識別子M i dによって暗号化される。暗号化装置36によって暗号化された暗号化電文E M i d（K u，K a）は回線を通じて要求元のエンドユーザに送信される。この処理が達成されると、ユーザプロファイル37に課金処理の指示が伝えられ、要求元のエンドユーザに対して課金を実施される。

【0038】図9はエンドユーザ側における処理の手順を示す説明図である。この図において、センタから送信された暗号化電文E M i d（K u，K a）を受信すると、まず、そのうちのMO媒体に関する暗号化電文E M i d（K u）をMO媒体40の所定の領域41に書き込む。そして、受信された暗号化電文E M i d（K u，K a）は復号装置51に入力される。復号装置51はMO媒体40の記憶媒体個別識別子M i dを使って暗号化電文E M i d（K u，K a）を復号し、記憶媒体用変換鍵K uおよびマスタ媒体用変換鍵K aを出力する。復号されたマスタ媒体用変換鍵K aは復号装置52に復号鍵として入力され、記憶媒体用変換鍵K uは暗号化装置53に暗号鍵として入力される。まず、復号装置52は、C D-R O M60のソフトウェア個別識別子D I Dに対応する暗号化データE K a（D a t a）を読み込んでマスタ媒体用変換鍵K aにより復号し、平文のデータD a t aに戻して出力する。このデータD a t aは暗号化装置53に入力され、記憶媒体用変換鍵K uで再暗号化される。暗号化装置53で暗号化された暗号化データE K u（D a t a）はMO媒体40に書き込まれる。

【0039】次に、以上の手順でMO媒体40に書き込まれた、このMO媒体40に固有の識別子およびセンタのマスタ鍵に基づく変換鍵による暗号化データE K u（D a t a）を利用する場合の処理手順について説明する。

【0040】図10はコピーされたデータの利用処理手順を示す説明図である。MO媒体40は、書き換え可能な領域の中の領域41に暗号化電文E M i d（K u）が記憶され、書き換え不可能な領域42に記憶媒体個別識

別子M i dが記憶され、それ以外の領域の一部にコピーされた暗号化データE K u (D a t a)が記憶されている。ここで、暗号化データE K u (D a t a)を利用する場合は、まず、M O媒体40上の記憶媒体個別識別子M i dおよび暗号化電文E M i d (K u)が読み出されて復号装置54に入力される。復号装置54は記憶媒体個別識別子M i dを用いて暗号化電文E M i d (K u)を復号し、記憶媒体用変換鍵K uを出力する。復号装置55は記憶媒体用変換鍵K uを復号鍵として使用し、M O媒体40から読み出された暗号化データE K u (D a t a)を復号して、平文のデータD a t aを出力する。このデータD a t aはエンドユーザの端末であるパーソナルコンピュータのメインメモリ上に展開され、これがプログラムならば実行され、辞書データならば検索するなどして利用される。

#### 【0041】

【発明の効果】以上説明したように本発明では、マスタ媒体のコピー対象データの識別子およびコピー先記憶媒体の識別子の情報から署名を生成する署名生成手段をセンタ側に備え、エンドユーザ側では署名生成手段によって生成された署名をコピー先記憶媒体に書き込む署名書込手段と、エンドユーザ側で生成した検証用の署名とコピー先記憶媒体に書き込まれた署名とを比較する署名生成比較手段と、比較結果によってマスタ媒体のコピー対象データをコピー先記憶媒体に書き込むデータコピー手段を備えるように構成した。このため、センタは、コピー先記憶媒体の識別子の情報に対してこれと対応する署名を発行するだけでよく、また、コピー先記憶媒体の製造工場と連携しての識別子情報の管理というようなことも必要なく、コピー先記憶媒体を製造する工場やこれを販売する店において、コピー先記憶媒体の在庫管理を不

要にすることができる。

#### 【図面の簡単な説明】

【図1】本発明のソフトウェアコピー処理装置の原理構成を示す図である。

【図2】ソフトウェアコピー処理装置の処理の流れを示すフローチャートである。

【図3】C D-R O MおよびM O媒体の構成を示す図である。

【図4】著作権保護ソフトウェアのコピー処理の手順を示す図である。

【図5】署名処理装置の構造例を示す図である。

【図6】コピーされたデータに含まれるソフトウェアのプログラムの実行処理手順を示す説明図である。

【図7】ソフトウェアコピー処理装置の別のコピー処理の流れを示すフローチャートである。

【図8】センタ側における処理の手順を示す説明図である。

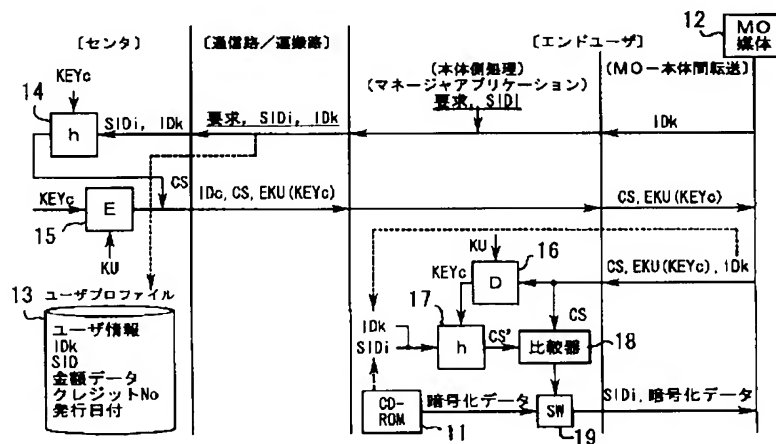
【図9】エンドユーザ側における処理の手順を示す説明図である。

【図10】コピーされたデータの利用処理手順を示す説明図である。

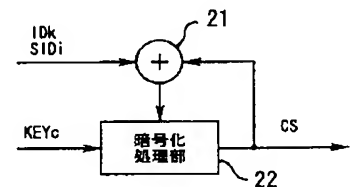
#### 【符号の説明】

- 1 マスタ媒体
- 2 コンテンツ識別子読取手段
- 3 コピー先記憶媒体
- 4 記憶媒体識別子読取手段
- 5 センタ
- 6 署名生成手段
- 7 署名書込手段
- 8 署名生成比較手段
- 9 データコピー手段

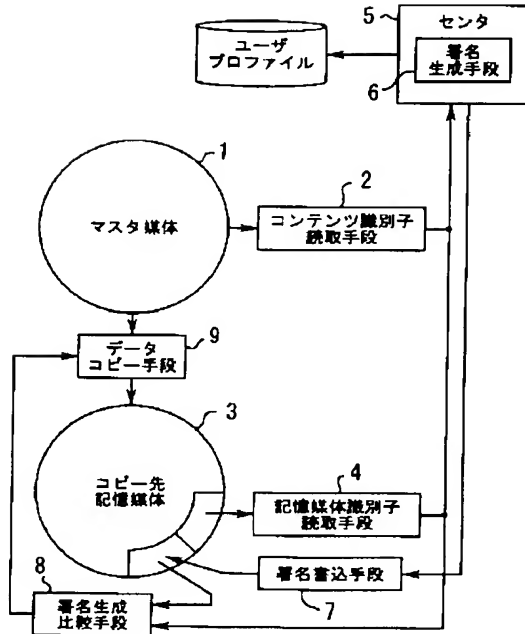
【図4】



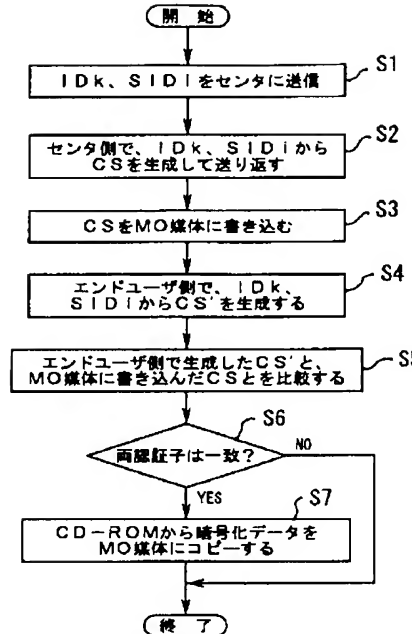
【図5】



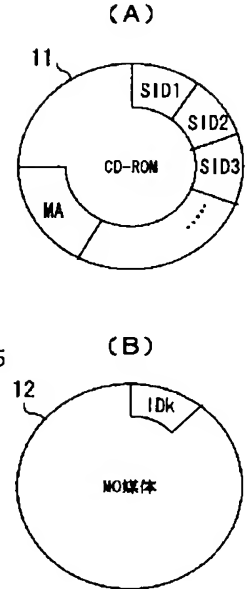
【図1】



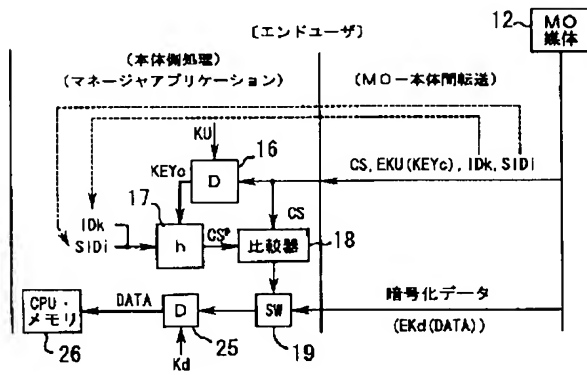
【図2】



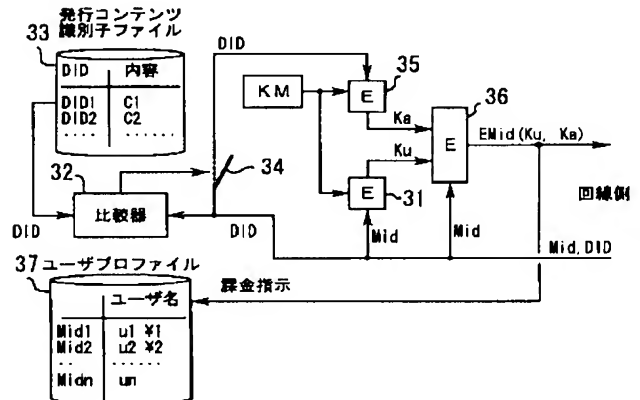
【図3】



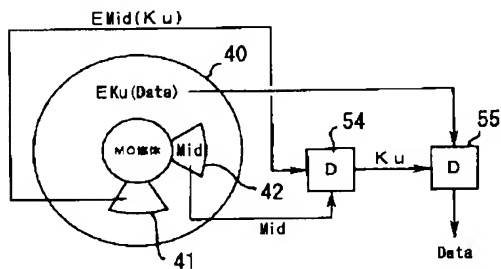
【図6】



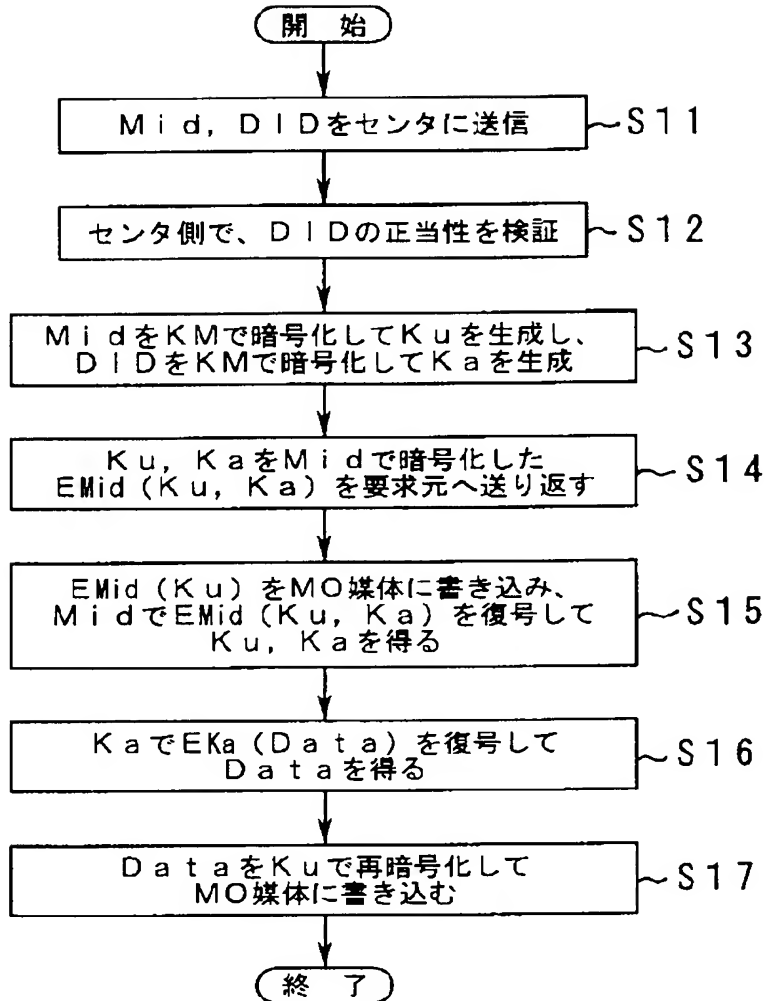
【図8】



【図10】



【図7】



【図9】

